UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/738,243	12/15/2000	Lok Yan Leung	AUS920000814US1	2747

35525 7590 08/26/2005

IBM CORP (YA)
C/O YEE & ASSOCIATES PC
P.O. BOX 802333
DALLAS, TX 75380

EXAMINER	
COLIN, CARL G	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 08/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/738,243	LEUNG ET AL.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 June 2005* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,8-10,12-14,19,26-29,33-35,37-39,42 and 43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,8-10,12-14,19,26-29,33-35,37-39,42 and 43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 December 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 6/15/2005, applicant amends claims 1, 9, 10, 12, 13, 19, 26, 33, 34, 35, 37, 38, 42, and 43, and cancels claims 5-7, 11, 15-18, 20-25, 30-32, 36, 40-41, and 44-46. The following claims 1-4, 8-10, 12-14, 19, 26-29, 33-35, 37-39, and 42-43 are presented for examination.

2. In response to communications filed on 6/15/2005, the objection to the specification has been withdrawn.

3. Applicant's remarks, pages 9-12, filed on 6/15/2005, with respect to the rejection of claims 1-5, 8-14, 17-19, 26-30, 33-39, 42-44 have been fully considered but they are not persuasive. Applicant argues that the reference does not teach any type of key conversion because the key is not readable or accessible outside the card. Examiner respectfully disagrees. For example, column 5, line 65 through column 5, line 6 discloses key store manager obtaining private key data from a smartcard; column 7, lines 32-33 recite "other devices external to the smartcard can read or obtain private key"; column 8, lines 30-37 discloses "alternatively, public key may be obtained from user A's smart card" for performing cryptographic operations. Column 2, lines 28-35 discloses "in both a smartcard based approach and host encryption based approach" (hardware process and software process) "there must be provided encryption scheme specific application programming interfaces to the system applications that allow such

applications to obtain private key and user data from the appropriate resource whether it is the key store manager or the smartcard. Therefore, Samar clearly discloses software key made available into hardware form and hardware key translating into software form that meets the recitation of key conversion from software to hardware form and vice versa. Applicant has amended claims 1, 9, 10, 12, 13, 19, 26, 33, 34, 35, 37, 38, 42, and 43. Upon further consideration, a new ground of rejection is made in view of Lockhart et al. The use of Lockhart in the rejection is to fully support the key conversion already disclosed by Samar. Examiner respectfully asserts that Samar either alone or in combination with Lockhart discloses the amended claimed limitations. Applicant is provided with other prior arts below 5,651,067 to Ahrens et al and 6,523,119 to Pavlin et al that clearly disclose the use of key conversion.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4.1 **Claims 1-4, 8-10, 12-14, 19, 26-29, 33-35, 37-39, and 42-43** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,778,072 to **Samar** in view of US Patent 6,393,565 to **Lockhart et al**.

4.2 **As per claims 1, 8, 26, 33, 42, and 43, Samar** discloses a method and system in a data processing system for executing cryptographic operations comprising bus system, memory connecting to the bus, and communication unit connecting to the bus for sending receiving data and processor unit for performing the invention (see fig. 1): responsive to a request to perform a cryptographic operation, dynamically selecting whether to perform an encryption operation with a smart card or an encryption operation using an encryption service based on whether the user has a smart card or based on the encryption scheme used, for example (see column 4, line 66 though column 5, line 18 and column 5, lines 47-62 and column 7, lines 10-33 and column 8, lines 38-61) that meets the recitation of dynamically selecting between one of a software process and a hardware process within the data processing system for performing the cryptographic operation based on a policy to form a selected process. **Samar** discloses the limitation of performing the cryptographic operation using the selected process, for example (see column 7, line 10-36 and column 8, lines 38-61); wherein the cryptographic operation is an encryption of data using a key, for example (see column 7, lines 10-36 and column 8, lines 38-61). **Samar** discloses the step of performing the cryptographic operation includes converting the software key to a form usable by the smartcard if the key is in an unusable form by the smartcard process (column 7, line 10 through column 9, line 5); column 5, line 65 through column 5, line 6 discloses key store manager obtaining private key data from a smartcard; column 7, lines 32-33

recite "other devices external to the smartcard can read or obtain private key"; column 8, lines 30-37 discloses "alternatively, public key may be obtained from user A's smart card" for performing cryptographic operations; column 2, lines 28-35 discloses "in both a smartcard based approach and host encryption based approach" (hardware process and software process) "there must be provided encryption scheme specific application programming interfaces to the system applications that allow such applications to obtain private key and user data from the appropriate resource whether it is the key store manager or the smartcard; that meets the recitation of wherein the key is a software key and the selected process is the hardware process and the step of converting the key comprises converting the software key into a hardware form useable by the hardware process for performing the cryptographic operation.

Samar discloses the step of performing the cryptographic operation includes: a hardware key can be obtained from the smartcard and be made usable by the software process when key is in an unusable form by the software process as disclosed in column 2, lines 28-35 discloses "in both a smartcard based approach and host encryption based approach" (hardware process and software process) "there must be provided encryption scheme specific application programming interfaces to the system applications that allow such applications to obtain private key and user data from the appropriate resource whether it is the key store manager or the smartcard; also see column 1, lines 15-37 where the public key can also be made available to a smart card or an encrypted private key can also be made available to the smart card since it is secured in encrypted form; that meets the recitation of wherein the key is a hardware key and the selected process is the software process and further comprising: converting the hardware key into a software form useable by the software process for performing the cryptographic operation.

Samar discloses the flexibility of using either software encryption service or hardware process by having an application interface interoperating with both system to provide the necessary data or keys for performing public/private key cryptographic operations (column 3, line 52 through column 4, line 7 and column 8, line 61 through column 9, line 5).

Lockhart et al in an analogous art teaches a data management system comprising bus system, memory connecting to the bus, and communication unit connecting to the bus for sending receiving data (see drawings 1-2) and processor unit connected to the bus system and further comprising a cryptographic data manager that interfaces with a hardware token such as a smartcard translating hardware key from the smart card to make it available to a software process due to limited capacity of the hardware token and also converting newly generated software key to a hardware form to be made available to the smartcard (see column 3, line 20 through column 4, line 14; column 4, line 45 through column 5, line 3; and column 5, line 49 through column 6, line 18). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Samar** as Samar suggests that the mode of storage of the private key depends on the security and ease of use requirements of the system and the user (column 1, lines 32-36) to implement key conversion wherein the key is a software key and the selected process is the hardware process and the step of converting the key comprises converting the software key into a hardware form useable by the hardware process for performing cryptographic operation and wherein the key is a hardware key and the selected process is the software process and further comprising: converting the hardware key into a software form useable by the software process for performing cryptographic operation as taught by **Lockhart et al.** One skilled in the art would have been lead to make such a modification

because it provides flexibility of using either a hardware process or software process for encryption as suggested by Samar and it also provides key updating in the smartcard if the public/private key pair has expired or compromised as suggested by **Lockhart et al** (column 1).

As per claims 2, 19, and 27, Samar discloses the limitation of wherein the policy includes selecting the one based on available resources to perform the cryptographic operation, wherein the identified available resources include available processing resources and memory, for example (see column 3, line 63 through column 4, line 7 and abstract).

As per claims 3, 10, 28, and 35 Samar discloses the limitation of wherein the policy includes selecting the software process that meets the recitation of selecting one resulting in a fastest completion of the cryptographic operation, for example (see column 8, lines 54-61).

As per claims 4 and 29, Samar discloses the limitation of wherein the selecting step includes: selecting the one using a preference associated with the request, for example (see column 3, line 63 through column 4, line 7).

As per claims 9 and 34, Samar discloses the limitation of wherein the policy comprises a set of rules used to minimize available resources consumed in performing the cryptographic operation, for example (see column 3, line 45 through column 4, line 7).

As per claims 12 and 37, Samar discloses the limitation of wherein the cryptographic operation is one of a message digest and a public-private key encryption, for example (see column 8, lines 18-61).

As per claims 13, 14, 38 and 39, Samar discloses the limitation of wherein the request is received from the application using an application program interface call made by the application, for example (see column 7, lines 10-30).

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the art discloses the use of key conversion from software key to hardware key and hardware key to software key.

US Patents: 5,651,067 Ahrens et al ; 6,523,119 Pavlin et al.

5.1 Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

5.2 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cc

Carl Colin
Patent Examiner
August 18, 2005

Primary Examiner
AU 2131
8/19/05